STATE OF MAINE
PUBLIC UTILITIES COMMISSION

Docket No. 2000-849

April 15, 2003

MAINE PUBLIC UTILITIES COMMISSION
Inquiry Regarding the Entry of Verizon-Maine
Into The InterLATA Telephone Market Pursuant
To Section 271 of Telecommunication
Act of 1996

EXAMINER'S REPORT

NOTE: This Examiner's Report is written in the form of an Order; however, it is the Advisors recommendation only and does not constitute formal Commission action. Parties may file exceptions to this Report by close of business on April 24, 2003. We anticipate that the Commission will consider this case at its deliberative session on Tuesday, April 29, 2003.

I. SUMMARY

In this Order we deny Verizon Maine's (Verizon or the Company) request for a waiver of certain wholesale service performance metric results for the month of January 2003. We find that Verizon has not met the standards contained in the Performance Assurance Plan (PAP) for granting a waiver for "situations beyond Verizon ME's control" from performance metrics with absolute standards. While Verizon's Operational Support Systems (OSS) faced a serious situation with the attack by an Internet "worm" on Saturday, January 25, 2003, the Company has not proven that it took sufficient steps to prevent this type of occurrence from having a major effect on its systems. Therefore, the rebate owed to Competitive Local Exchange Carriers (CLECs) is not reduced.

II. BACKGROUND

On March 17, 2003, Verizon filed a request for waiver of certain wholesale service performance metric results for January 2003 that otherwise would be included in

the calculation of monthly bill credits to CLECs under the provisions of the PAP. Verizon asserted that three PAP pre-order OSS availability metrics were adversely affected because on Saturday, January 25, 2003, Verizon's systems were attacked by an Internet worm, which came to be known as the "Slammer Worm," and the attack prevented Verizon from meeting the absolute standards for three PAP wholesale measures for pre-order availability. The Company states that the worm attack is an event that was beyond its control, and it negatively affected its ability to meet the absolute standards of three wholesale metrics. Under the terms of the PAP, Verizon calculated the rebate owed to CLECs for January 2003 at approximately $62,000, but if the waiver were granted, the rebate would be reduced to approximately $18,000.

Verizon states that early in the morning of January 25, 2003, an unknown source began flooding the Internet with vast amounts of traffic. The additional traffic was caused by the propagation of a worm, a type of virus that does not create or destroy files, but rather simply scans the servers that it attacks for other vulnerable devices, then sends itself to the new device, where the process repeats itself quickly. The scanning and propagation actions created huge amounts of network and Internet traffic, causing congestion on the affected systems, including Verizon's, on the morning of January 25th. Shortly after Verizon's network managers detected the presence of the worm, they began "defensive tactics" to isolate the Verizon network port that was receiving the traffic, and they isolated Verizon's internal data networks into segments.

Later during the morning of January 25th, Verizon observed very high utilization rates on its Internet connections, which led the Company's network managers to conclude that its systems were under attack from the Internet. Verizon decided that an

external quarantine process was necessary to ensure the safety of its networks and systems. At that time, the wholesale OSS interfaces were brought down in order to speed isolation and recovery from the worm attack. Verizon notified all CLECs by email of the event, and it contacted by phone the one CLEC that was attempting to use the on-line interface. In order to inspect, identify and remove infected devices from service, and where appropriate to patch, test and reconnect devices, Verizon kept its OSS network interfaces off-line until about 6:00 PM on Sunday, January 26, 2003.

In calculating its performance under the pre-order system availability metric, Verizon recorded all day Saturday, a prime time period, as having zero availability. This resulted in the three OSS Interface Availability metrics for prime time (EDI, COBRA and WEB GUI) having performance results below the standard of 99.5%. Based on the weighted scores resulting from the substandard performance, Verizon owed penalties totaling $44,195 in the Mode of Entry and Critical Measures categories. If the results for Saturday, January 25th, were excluded from the calculation, the monthly results would meet the absolute standards for the measures.

Verizon seeks a waiver from the performance metrics for the month of January 2003, because it asserts that the attack created a situation that was beyond Verizon's control, and that Verizon acted in a proactive manner in attempting to defend itself from the attack. In its waiver request, Verizon also describes its computer security practices, particularly those concerned with obtaining, evaluating, testing and deploying software "patches" that are designed to enhance network performance and security. Patches are usually provided by software suppliers in response to identified shortcomings in the active software. Verizon claims that installation of software patches "is not a trivial

function," but rather requires a considerable amount of testing and evaluation to ensure that unforeseen interoperability problems do not occur. In addition, the installation of any particular patch may require, as a pre-condition, the installation of prior patches or intermediate software releases. Verizon asserts that patch management represents a very serious challenge for most large businesses.

Verizon claims that at the time the Slammer Worm hit on January 25th, it had not yet applied a patch to all of its systems that would fend off the virus. Verizon further asserts that media accounts in the aftermath of the worm attack indicated that Verizon's experience was fairly typical in dealing with this occurrence. The Company says that while Microsoft had released patches that addressed the specific vulnerability exploited by the Slammer Worm, it is only in hindsight that specific patches to address the problem can be identified.

Verizon asserts that the Slammer Worm attack is similar to other events for which the Commission has granted waivers of applicable service quality measures. Verizon claims that it took reasonable precautions to protect its computer systems form attack. Verizon believes that by isolating its systems, it was able to avoid major damage to its network and systems, and it was able to restore service as quickly as possible. The Company asserts that the threshold question is whether Verizon exercised reasonable, prudent judgment, consistent with industry practices, in operating its "cyber facilities." Verizon, therefore, believes it has met the standards set forth in the PAP and demonstrated that it is entitled to a waiver.

Responsive comments were filed by AT&T Communications of New England (AT&T) and WorldCom, and both parties oppose granting Verizon's waiver request.

The parties agree with Verizon that software patch management is an important and complex task. The parties assert, however, that Verizon had sufficient notice of a software patch for the type of worm attack that occurred on January 25th, but it failed to test and install the patch in a timely manner. AT&T also asserts that the fact that Verizon was able to test and deploy the patch in less than two days after the incident strongly suggests that the patch could have been deployed prior to the attack.

Further, AT&T asserts that Microsoft uses a four-part rating system for Security Bulletins it issues about software vulnerabilities, and the bulletins and associated patches related to the Slammer Worm problem were given a "Critical" rating, because they were and are considered to pose the most serious threat to Internet security. Microsoft apparently recommends that patches with Critical (and "Important", the second highest warning level) ratings should be "applied in an especially timely manner." AT&T asserts that Microsoft posted Security Bulletins related to the Slammer Worm vulnerability on October 2 and 16, 2002, more than three months prior to the actual attack. Both Bulletins carried a "Critical" label, but Verizon apparently chose not to install either of the patches provided.

AT&T also notes that Verizon generally shuts down its OSS every Sunday (non-prime time) for testing and installation of software upgrades and patches. Thus, Verizon can conduct these activities without suffering PAP consequences for sub-standard performance. AT&T asserts that from October 16, 2002, until the worm attack on January 25, 2003, Verizon had 15 occasions on which it could have tested and deployed the patch promulgated by Microsoft.

AT&T argues that the waiver provisions in the PAP are directed toward "events that are truly exceptional and beyond Verizon Maine's control, not to events that are mundane and common to a number of companies." AT&T also asserts that it did not experience the kind of problems that Verizon did, nor were there material impacts to AT&T's command and control systems or customer care services. AT&T also asserts that, anecdotally, it has heard that other telecommunications carriers did not experience the kind or magnitude of problems that Verizon did.

WorldCom opines that Verizon's request should be denied because the Company has failed to meet the waiver standards contained in the PAP. While WorldCom says it appreciates the complexities involved in network and systems security, it asserts that the Slammer Worm attack was not, as Verizon claims, an unforeseeable event that was beyond Verizon's control. WorldCom asserts as early as June 24, 2002, Microsoft issued a security bulletin warning of the dangers from an attack of this type on the type of servers that Verizon uses in its systems. The bulletin in question also recommended use of a particular kind of software patch to prevent exploitation of networks by a worm. WorldCom also indicates that the bulletin had a "critical" rating for the danger posed by a worm attack.

WorldCom asserts that Verizon should reasonably be expected to keep abreast of critical vulnerabilities to its network and take all reasonable actions to defend against such attacks. While the Slammer Worm attack itself was beyond Verizon's control, protecting its systems was not. WorldCom claims that it was able to defend itself against the Slammer Worm attack, and Verizon should have been expected to do likewise, particularly in light of its obligations under the PAP. Thus, Verizon's failure to

install the appropriate patches is evidence that it failed to act in a reasonable and prudent manner. Verizon, not CLECs, should be held accountable for its failure, and Verizon's waiver request should be denied.

III. DISCUSSION AND FINDINGS

The description of the grounds for filing a waiver request and of the standards for granting the request are contained in PAP Section II (J), beginning at page 23 of the June 25, 2002, version of the PAP. The current request is based on the third ground for filing a waiver, relating "to situations beyond Verizon ME's control that negatively affect its ability to satisfy only those measures with absolute standards." Further, according to the PAP, "Any petition pursuant to this provision must demonstrate clearly and convincingly the extraordinary nature of the circumstances involved, the impact the circumstances had on Verizon's service quality, why Verizon ME's normal, reasonable preparations for difficult situations proved inadequate, and the specific days affected by the event. " The waiver petition must be filed within 45 days of the end of the month in which the event occurred. Also, "The Commission will determine which, if any, of the daily and monthly results should be adjusted in light of the extraordinary event cited, and will have full discretion to consider all available evidence submitted. Insufficient filings may be dismissed for failure to make a *prima facie* showing that relief is justified."

While the Slammer Worm attack was certainly a serious occurrence, we agree with WorldCom that it is not the type of extraordinary event that is contemplated by the waiver section of the PAP. While they do not appear on a frequent basis, unfortunately Internet viruses and worms have been promulgated on numerous occasions in the past,

and the Slammer Worm is just the latest version of the genre. The fact that Microsoft more or less regularly issues security bulletins is evidence that events of this type occur and are an all too frequent occurrence that requires constant vigilance.

Next, we must analyze Verizon's actions prior to the attack and its response to the circumstances after the attack began. There is no evidence to question the Company's actions in responding to the Slammer Worm attack of January 25, 2003. Once the problems associated with the attack became evident, Verizon apparently pursued the only prudent action available for its defense: a complete shutdown of its OSS.

With respect to its ex ante actions taken to prevent or minimize worm attacks, we find that Verizon did not take all reasonable and prudent steps available to it. According to AT&T and WorldCom, Microsoft initially notified network administrators of a potential problem with the Slammer Worm at least six months before the attack actually occurred, and it issued "Critical" security bulletins and associated software patches at both six and three months intervals prior to the event. Despite these warnings, Verizon apparently chose not to install the appropriate patch. In support of its request, the Company describes only in very general terms the process it uses to test, evaluate and eventually install the numerous software patches that are made available by various software vendors, such as Microsoft. By failing to provide specific evidence about its knowledge and analysis of the vulnerabilities of its systems to the Slammer Worm, Verizon failed to make the clear and convincing demonstration required in § II (J) of the PAP. We find the assertions of AT&T and WorldCom that companies had sufficient warning about system vulnerabilities posed by the Slammer Worm and that AT&T and WorldCom were

largely unaffected by the worm attack because they installed the Microsoft patch to be credible. Also, we find that Verizon failed to act in a reasonable and timely manner to institute preventive actions. Thus, Verizon should be held accountable for its failure.

IV. CONCLUSION

For the reasons stated above, Verizon Maine's request for a waiver of certain service quality results under the PAP for January 2003, is DENIED.

BY ORDER OF THE HEARING EXAMINER

_____

Trina M. Bragdon